(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－247111
（Ｐ2002－247111Ａ）
(43)公開日　平成14年８月30日（2002.8.30）

(51)Int.Cl.'	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ04Ｌ　12/66		Ｈ04Ｌ　12/66	Ｂ	5Ｂ085
Ｇ06Ｆ　15/00	330	Ｇ06Ｆ　15/00	330Ａ	5Ｊ104
Ｈ04Ｌ　9/32		Ｈ04Ｌ　9/00	675Ｄ	5Ｋ030

審査請求　未請求　請求項の数16　ＯＬ　（全９頁）

(21)出願番号　特願2001－43512(Ｐ2001－43512)

(22)出願日　平成13年２月20日(2001.2.20)

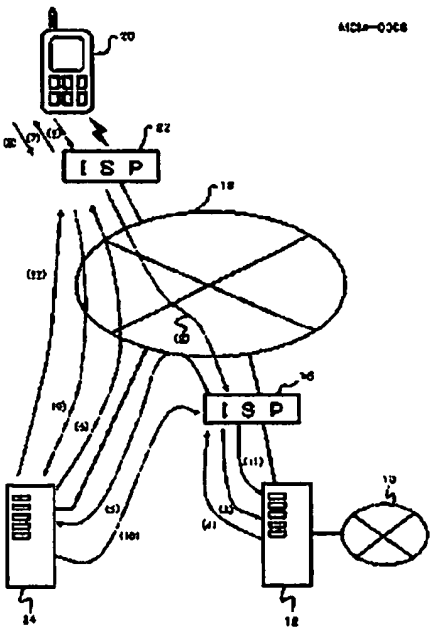
(71)出願人　595161887
エム・シー・エムジャパン株式会社
東京都世田谷区三軒茶屋２－11－22　サンタワーズセンタービル
(72)発明者　斉藤　亨
東京都世田谷区三軒茶屋２丁目11番22号　サンタワーズセンタービル　エム・シー・エムジャパン株式会社内
(74)代理人　100109014
弁理士　伊藤　充

Ｆターム(参考)　5Ｂ085 ＡＡ01 ＡＥ02 ＡＥ04
5Ｊ104 ＡＡ07 ＫＡ01 ＭＡ02 ＰＡ07
5Ｋ030 ＧＡ15 ＨＡ08 ＨＣＤ1 ＨＩ03 ＨＤ06
ＫＡ01 ＫＡ04 ＫＡ06 ＬＢ02 ＬＣ13

(54)【発明の名称】　不正アクセス防止方法及びセキュリティ管理装置及びゲートウェイ装置及び端末装置

(57)【要約】
【課題】　プライベートなネットワークに対する外部からの不正アクセスを防止しうる方法及びその方法を実現する装置を提供する。
【解決手段】　端末２０から家庭内ネットワーク１０に対するパケットが送信されると、ゲートウェイ装置１２は、パケットのパケット情報と、自己認証データとを、セキュリティ管理装置２４に送信する。セキュリティ管理装置２４は、パケットの送信者に対して認証データを要求する。端末２０は要求に応じて認証データを送信する。セキュリティ管理装置２４は送られてきた認証データに基づき、送信者が正当な権利を有するか否か検査し、正当な権利を有していれば、ゲートウェイ装置１２に対して、フィルタリングの解除命令を出す。一方、不正なアクセスであると判断した場合は、第２のＩＳＰ２２に対して、警告を通知する。このようにして、アクセスの管理を外部に委託することができる。

図1



1

【特許請求の範囲】

【請求項１】　外部ネットワークと内部ネットワークとをゲートウェイ装置で接続し、前記外部ネットワーク側から、前記内部ネットワーク側の装置に対する不正なアクセスを防止する不正アクセス防止方法において、

前記外部ネットワーク側から、前記内部ネットワーク内の装置に対してデータパケットが送信されてきた場合に、前記データパケットのパケット情報と、前記ゲートウェイ装置の自己認証データと、を前記外部ネットワーク上のセキュリティ管理装置に送信するパケット情報送信ステップと、

前記セキュリティ管理装置が、前記パケット情報に基づき、前記データパケットの送信者に送信者側認証データを要求する要求ステップと、

前記要求に応じて、前記送信者が前記送信者側認証データを前記セキュリティ管理装置に送信する送信者側認証データ送信ステップと、

前記送信されてきた送信者側認証データと、前記ゲートウェイ装置の自己認証データと、に基づき、前記送信者が前記内部ネットワークへのアクセスを許可されているか否かを判断する認証ステップと、

前記認証ステップの結果、前記送信者が前記内部ネットワークへのアクセスを許可されている場合には、前記セキュリティ管理装置は、前記ゲートウェイ装置に対して、前記データパケットの内部ネットワークへの流入を許可するよう命令する命令ステップと、

を含むことを特徴とする不正アクセス防止方法。

【請求項２】　請求項１記載の不正アクセス防止方法において、

前記認証ステップの結果、前記送信者が前記内部ネットワークへのアクセスを許可されていない場合には、前記セキュリティ管理装置は、前記送信者を管理する管理者に対して、警告を通知する警告通知ステップ、

を含むことを特徴とする不正アクセス防止方法。

【請求項３】　請求項１記載の不正アクセス防止方法において、

前記要求ステップを実行した後、所定期間内に前記送信者側認証データが送信されてこなかった場合に、前記セキュリティ管理装置は、前記送信者を管理する管理者に対して、警告を通知する第２警告通知ステップ、

を含むことを特徴とする不正アクセス防止方法。

【請求項４】　請求項１、２又は３記載の不正アクセス防止方法において、

前記外部ネットワークはインターネットであり、前記内部ネットワークは家庭内ネットワークであることを特徴とする不正アクセス防止方法。

【請求項５】　請求項１、２又は３記載の不正アクセス防止方法において、

前記パケット情報は、前記データパケットの送信者のＩＰアドレス又はＴＣＰ情報又はＵＤＰアクセスポート番号のいずれかであることを特徴とする不正アクセス防止方法。

2

【請求項６】　請求項２又は３記載の不正アクセス防止方法において、

前記送信者を管理する前記管理者は、前記送信者が利用するインターネットサービスプロバイダであることを特徴とする不正アクセス防止方法。

【請求項７】　ネットワークを介して接続された他の通信装置の管理を行うセキュリティ管理装置であって、

前記ネットワークと接続するインターフェース手段と、

前記他の通信装置に対してアクセスを許可された者の認証データが記載された表を記憶する記憶手段と、

前記他の通信装置から、前記他の通信装置にデータパケットを送信した送信者の認証を依頼された場合に、前記送信者にその者の認証データの送付を依頼し、送付されてきた前記認証データが、前記表に記載されているか否かを検査し、記載されている場合には、前記他の通信装置にアクセスを許可する旨の命令を発する制御手段と、

を含むことを特徴とするセキュリティ管理装置。

【請求項８】　請求項７記載のセキュリティ管理装置であって、

前記制御手段は、前記送付されてきた認証データが前記表に記載されていない場合には、前記送信者の管理者に警告を通知することを特徴とするセキュリティ管理装置。

【請求項９】　請求項７記載のセキュリティ管理装置であって、

前記制御手段は、前記認証データの送付を依頼した後、所定期間内に前記認証データが送信されてこなかった場合に、前記送信者の管理者に警告を通知することを特徴とするセキュリティ管理装置。

【請求項１０】　請求項７、８又は９記載のセキュリティ管理装置において、

前記ネットワークはインターネットであり、前記他の通信装置はゲートウェイ装置であることを特徴とするセキュリティ管理装置。

【請求項１１】　請求項８又は９記載のセキュリティ管理装置において、

前記管理者は、前記送信者が接続するインターネットサービスプロバイダであることを特徴とするセキュリティ管理装置。

【請求項１２】　外部ネットワークと内部ネットワークとを接続するゲートウェイ装置であって、

前記外部ネットワークと接続する第１インターフェース手段と、

前記内部ネットワークと接続する第２インターフェース手段と、

前記外部ネットワークから前記内部ネットワークに向かうデータパケットのフィルタリングを行うフィルタリング手段と、

3

前記フィルタリング手段の制御を行う制御手段であって、前記外部ネットワークから前記内部ネットワークに向かうデータパケットが送信されてきた場合に、前記パケットのパケット情報と、ゲートウェイ装置の自己認証データとを他の管理装置に送信し、この管理装置からフィルタリングを解除する旨の命令が送信されてきた場合に、前記フィルタリング手段のフィルタリングを解除し、前記データパケットを前記内部ネットワークへ流すことを許可する制御手段と、
を含むことを特徴とするゲートウェイ装置。
【請求項１３】　請求項１２記載のゲートウェイ装置において、
前記外部ネットワークは、インターネットであり、前記内部ネットワークは家庭内ネットワークであることを特徴とするゲートウェイ装置。
【請求項１４】　請求項１２記載のゲートウェイ装置において、
前記パケット情報は、前記データパケットの送信者のＩＰアドレス又はＴＣＰ情報又はＵＤＰアクセスポート番号のいずれかであることを特徴とするゲートウェイ装置。
【請求項１５】　請求項１２記載のセキュリティ管理装置において、
前記管理装置は、前記外部ネットワークを介して接続しうるセキュリティ管理装置であることを特徴とするゲートウェイ装置。
【請求項１６】　ネットワークに接続可能な端末装置において、
前記ネットワークに接続するインターフェース手段と、
前記ネットワークを介して、他の管理装置から本端末装置側の認証データの送信を要求された場合に、前記認証データを前記他の管理装置に対して送信する制御手段と、
を含むことを特徴とする端末装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、所定のネットワークに対する不正アクセスを防止する方法に関する。さらに、この方法を実現する各種通信機器に関する。
【０００２】
【従来の技術】近年、ネットワークが発達し、家庭内においてもいわゆる家庭内ネットワークが広く利用されている。この家庭内ネットワークにおいては、複数の情報家電製品が互いに接続され、情報の共有等が実現されている。また、この家庭内ネットワークは外部のインターネット等に接続されている場合も多い。
【０００３】さて、この家庭内ネットワークの利用者は、外部からその家庭内ネットワークにアクセスできれば便利である。たとえば、インターネット上からこの家庭内ネットワーク内の情報家電製品にアクセスできれば

4

家庭内ネットワークの情報を外部から取り出すことができれば、利便性の高い運用が可能である。特に、近年はインターネットにアクセス可能な携帯電話等が広く普及しており、そのような携帯電話からインターネットを介して家庭内ネットワークにアクセスできれば一層利便性に富む運用が可能である。
【０００４】
【発明が解決しようとする課題】しかしながら、外部から家庭内ネットワークへのアクセスを無制限に認めたのでは、悪意の第三者が家庭内ネットワークに侵入し、その家庭内のプライバシーの侵害等の問題を生じさせるおそれがある。
【０００５】そこで、家庭内ネットワークと外部のインターネット等との間にアクセスを監視する何らかの手段を講じることが望ましい。
【０００６】本発明はこのような課題に鑑みなされたものであり、その目的は、プライベートなネットワークに対する外部からの不正アクセスを防止しうる方法及びその方法を実現する装置を提供することである。
【０００７】
【課題を解決するための手段】上記課題を解決するために、本発明は、外部ネットワークと内部ネットワークとをゲートウェイ装置で接続し、前記外部ネットワーク側から、前記内部ネットワーク側の装置に対する不正なアクセスを防止する不正アクセス防止方法において、前記外部ネットワーク側から、前記内部ネットワーク内の装置に対してデータパケットが送信されてきた場合に、前記データパケットのパケット情報と、前記ゲートウェイ装置の自己認証データと、を前記外部ネットワーク上のセキュリティ管理装置に送信するパケット情報送信ステップと、前記セキュリティ管理装置が、前記パケット情報に基づき、前記データパケットの送信者に送信者側認証データを要求する要求ステップと、前記要求に応じて、前記送信者が前記送信者側認証データを前記セキュリティ管理装置に送信する送信者側認証データ送信ステップと、前記送信されてきた送信者側認証データと、前記ゲートウェイ装置の自己認証データと、に基づき、前記送信者が前記内部ネットワークへのアクセスを許可されているか否かを判断する認証ステップと、前記認証ステップの結果、前記送信者が前記内部ネットワークへのアクセスを許可されている場合には、前記セキュリティ管理装置は、前記ゲートウェイ装置に対して、前記データパケットの内部ネットワークへの流入を許可するよう命令する命令ステップと、を含むことを特徴とする不正アクセス防止方法である。
【０００８】このような構成によって、内部ネットワークにアクセスする正当な権利を有する者が内部ネットワークにデータパケットを送信することができる。
【０００９】また、本発明は、前記認証ステップの結果、前記送信者が前記内部ネットワークへのアクセスを

5

許可されていない場合には、前記セキュリティ管理装置は、前記送信者を管理する管理者に対して、警告を通知する警告通知ステップ、を含むことを特徴とする不正アクセス防止方法である。

【００１０】このような構成によって、不正なアクセスがあった場合に管理者に警告を発することができる。

【００１１】また、本発明は、前記要求ステップを実行した後、所定期間内に前記送信者側認証データが送信されてこなかった場合に、前記セキュリティ管理装置は、前記送信者を管理する管理者に対して、警告を通知する第２警告通知ステップと、を含むことを特徴とする不正アクセス防止方法である。

【００１２】このような構成によって、認証データが送信されない場合も、不正なアクセスがあったと判断し、管理者に警告を発することができる。

【００１３】また、本発明は、前記外部ネットワークはインターネットであり、前記内部ネットワークは家庭内ネットワークであることを特徴とする不正アクセス防止方法である。

【００１４】このような構成によって、インターネットから家庭内ネットワークに対する不正なアクセスを防止することができる。

【００１５】また、本発明は、前記パケット情報は、前記データパケットの送信者のＩＰアドレス又はＴＣＰ情報又はＵＤＰアクセスポート番号のいずれかであることを特徴とする不正アクセス防止方法である。

【００１６】このように、ＩＰアドレス等を利用することによって、パケットの送信者を特定することが可能である。

【００１７】また、本発明は、前記送信者を管理する前記管理者は、前記送信者が利用するインターネットサービスプロバイダであることを特徴とする不正アクセス防止方法である。

【００１８】このような構成によって、インターネットサービスプロバイダに対してそのユーザの中に不正なアクセスをする者がいることを知らせることが可能である。

【００１９】また、本発明は、ネットワークを介して接続された他の通信装置の管理を行うセキュリティ管理装置であって、前記ネットワークと接続するインターフェース手段と、前記他の通信装置に対してアクセスを許可された者の認証データが記載された表を記憶する記憶手段と、前記他の通信装置から、前記他の通信装置にデータパケットを送信した送信者の認証を依頼された場合に、前記送信者にその者の認証データの送付を依頼し、送付されてきた前記認証データが、前記表に記載されているか否かを検査し、記載されている場合には、前記他の通信装置にアクセスを許可する旨の命令を発する制御手段と、を含むことを特徴とするセキュリティ管理装置である。

6

【００２０】このような構成によれば、他の通信装置からパケットの送信者が正当な権利を有しているか否かの認証作業を委託されることができ、他の通信装置の管理負担を減少させることができる。

【００２１】また、本発明は、前記制御手段は、前記送付されてきた認証データが前記表に記載されていない場合には、前記送信者の管理者に警告を通知することを特徴とするセキュリティ管理装置である。

【００２２】このような構成によって、認証データが誤っていた場合に、管理者に警告を出すことができる。

【００２３】また、本発明は、前記制御手段は、前記認証データの送付を依頼した後、所定期間内に前記認証データが送信されてこなかった場合に、前記送信者の管理者に警告を通知することを特徴とするセキュリティ管理装置である。

【００２４】このような構成によって、認証データが所定期間内に送信されてこなかった場合も、不正なアクセスであると判断し、管理者に警告を出すことができる。

【００２５】また、本発明は、前記ネットワークはインターネットであり、前記他の通信装置はゲートウェイ装置であることを特徴とするセキュリティ管理装置である。

【００２６】このような構成によって、ゲートウェイ装置はインターネットからの不正なアクセスの判断を外部のセキュリティ管理装置に委託することができる。

【００２７】また、本発明は、前記管理者は、前記送信者が接続するインターネットサービスプロバイダであることを特徴とするセキュリティ管理装置である。

【００２８】このような構成によって、インターネットサービスプロバイダに対して、そのユーザの中に不正なアクセスをする者がいることを知らせることができる。

【００２９】また、本発明は、外部ネットワークと内部ネットワークとを接続するゲートウェイ装置であって、前記外部ネットワークと接続する第１インターフェース手段と、前記内部ネットワークと接続する第２インターフェース手段と、前記外部ネットワークから前記内部ネットワークに向かうデータパケットのフィルタリングを行うフィルタリング手段と、前記フィルタリング手段の制御を行う制御手段であって、前記外部ネットワークから前記内部ネットワークに向かうデータパケットが送信されてきた場合に、前記パケットのパケット情報と、ゲートウェイ装置の自己認証データとを他の管理装置に送信し、この管理装置からフィルタリングを解除する旨の命令が送信されてきた場合に、前記フィルタリング手段のフィルタリングを解除し、前記データパケットを前記内部ネットワークへ流すことを許可する制御手段と、を含むことを特徴とするゲートウェイ装置である。

【００３０】このような構成によって、パケットが正当な権利を有する者から送信されてきたものか否かの判断を外部に委託することができるゲートウェイ装置が得ら

れる。

【００３１】また、本発明は、前記外部ネットワークは、インターネットであり、前記内部ネットワークは家庭内ネットワークであることを特徴とするゲートウェイ装置である。

【００３２】このような構成によって、インターネットから家庭内ネットワークに対してなされるアクセスが正当なものか否かの判断を外部に委託することができる。

【００３３】また、本発明は、前記パケット情報は、前記データパケットの送信者のＩＰアドレス又はＴＣＰ情報又はＵＤＰアクセスポート番号のいずれかであることを特徴とするゲートウェイ装置である。

【００３４】このような構成によって、送信者を識別する情報としてＩＰアドレス等を利用することができる。

【００３５】また、本発明は、前記管理装置は、前記外部ネットワークを介して接続しうるセキュリティ管理装置であることを特徴とするゲートウェイ装置である。

【００３６】このような構成によって、セキュリティ管理装置は、内部ネットワーク内に対するアクセスをすることなく送信者が正当なものであるか否かの判断を行うことができる。

【００３７】また、本発明は、ネットワークに接続可能な端末装置において、前記ネットワークに接続するインターフェース手段と、前記ネットワークを介して、他の管理装置から本端末装置側の認証データの送信を要求された場合に、前記認証データを前記他の管理装置に対して送信する制御手段と、を含むことを特徴とする端末装置である。

【００３８】このような構成によって、認証データを管理装置に送信することができる。

【００３９】

【発明の実施の形態】以下、本発明の好適な実施の形態を図面に基づいて説明する。

【００４０】実施の形態１

図１には、本実施の形態１の通信システムの全体構成図が示されている。

【００４１】この図に示すように、本実施の形態１においては、家庭内ネットワーク１０は、ゲートウェイ装置１２を介して第１のインターネットサービスプロバイダ１６に接続している。そして、この第１のインターネットサービスプロバイダ１６を介して、インターネット１８に接続している。なお、図１においては、インターネットサービスプロバイダは「ＩＳＰ」と簡略した記載となっている。

【００４２】この家庭内ネットワーク１０に外部からアクセスしようとする者の端末２０は、第２のインターネットサービスプロバイダ２２に接続している。そして、この第２のインターネットサービスプロバイダ２２を介して、上記端末２０はインターネット１８に接続されている。第２のインターネットサービスプロバイダ２２も、図１においては、簡略した記載「ＩＳＰ」としている。以下、インターネットサービスプロバイダはしばしば「ＩＳＰ」と記す。

【００４３】家庭内ネットワークに外部から接続しようとする場合としては、その家庭の人が外から、家庭内部の情報を知りたいと思う場合が典型的な例としてあげられよう。

【００４４】この場合の端末２０は、たとえばパーソナルコンピュータが考えられる。また近年はインターネット１８に接続しうる携帯電話等も多く利用されているため、端末２０として携帯電話等の各種モバイル通信機器を利用することも考えられる。なお、端末２０は、本発明の「端末装置」に相当する。

【００４５】また、インターネット１８にはセキュリティ管理装置２４が接続されている。このセキュリティ管理装置２４は、ゲートウェイ装置１２毎に、そのゲートウェイ装置１２に対するアクセスを管理している。

【００４６】このセキュリティ管理装置２４には、自分が管理するゲートウェイ装置１２の自己認証データと、このゲートウェイ装置１２に対してアクセスが許可されている端末２０の認証データとを記載した表（データベース）が格納されている。このような表の概念図が図２に示されている。この図に示すように、この表は、ゲートウェイ装置１２毎に設けられた表であって、ゲートウェイ装置１２に対してアクセスが許可されている端末２０の認証データを記載した表である。

【００４７】なお、端末２０の認証データは、本発明の「送信者側認証データ」や「端末装置側の認証データ」に相当する。

【００４８】次に、端末２０から家庭内ネットワーク１０へのアクセスの動作について説明する。図３には、この際の動作の流れを表すフローチャートが示されている。

【００４９】まず、ステップＳ３－１においては、端末２０から家庭内ネットワーク１０に対するデータパケット（以下、単にパケットと呼ぶ）が送信される。このパケットは、まず第２のＩＳＰ２２に到着する（図１中（１）で示される）。続いて、パケットは、第２のＩＳＰ２２から、インターネット１８を通過して、第１のＩＳＰ１４に到着（図１中（２）で示される）する。そして、パケットは、第１のＩＳＰ１４から家庭内ネットワーク１０のゲートウェイ装置１２に到着する（図１中（３）で示される）。

【００５０】ステップＳ３－２においては、ゲートウェイ装置１２が、送られてきた上記パケットのパケット情報と、自己認証データとを、セキュリティ管理装置２４に送信する。このデータは、まず第１のＩＳＰ１６に到着し（図１中（４）で示される）、さらにインターネット１８を経由してセキュリティ管理装置２４に到着する（図１中（５）で示される）。

【００５１】ここで、自己認証データとは、ゲートウェイ装置１２が自己を表すためのデータであり、セキュリティ管理装置２４は、この自己認証データを用いてどのゲートウェイ装置１２であるかを識別することができる。また、パケット情報とは、上記パケットを送信した者（送信者）を特定できるデータであって、ＩＰアドレスや、ＴＣＰやＵＤＰのアクセスポート番号、又はパケットの内容等を利用することができる。

【００５２】ステップＳ３－３においては、セキュリティ管理装置２４が、上記パケット情報に基づきパケットの送信者を特定し、その送信者に対して認証データを要求する。この要求のメッセージはインターネット１８を介して第２のＩＳＰに到着し（図１中、（６）で示される）、第２のＩＳＰから端末２０に送信される（図１中、（７）で示される）。

【００５３】ステップＳ３－４からは、端末２０が上記要求に応じて認証データを送信するか否かによって、処理が分岐する。認証データを送信する場合には、ステップＳ３－５に処理が移行する。一方、何らかの理由により、認証データを送信できない場合は、セキュリティ管理装置２４は認証データを受信できない。セキュリティ管理装置２４が所定期間内に認証データを受信できなかった場合には、ステップＳ３－８に処理が移行する。

【００５４】ステップＳ３－５においては、端末２０からセキュリティ管理装置２４に対して認証データが送信される。この認証データはまず、端末２０から第２のＩＳＰに送られ（図１中、（８）で示される）、続いて、インターネット１８を介してセキュリティ管理装置２４に到着する（図１中、（９）で示される）。

【００５５】ステップＳ３－６においては、セキュリティ管理装置２４が送られてきた上記認証データに基づき、送信者がゲートウェイ装置１２に対してアクセスする権利を有するか検査される。この検査は、図２で説明した表を検索することによって実行される。まず、セキュリティ管理装置２４は、ゲートウェイ装置１２の自己認証データに基づき、そのゲートウェイ装置１２の表を見つけだす（図２）。次に、その表中に、パケットの送信者が送信してきた認証データが存在するか否か検査する。この検査の結果、表中に上記認証データが存在すれば、そのパケットの送信者はそのゲートウェイ装置１２を介して家庭内ネットワーク１０にアクセスする正当な権利を有していると判断し、ステップＳ３－７に処理が移行する。一方、上記表中に認証データが存在しない場合には、そのパケット送信者は正当な権利を有していないと判断し、ステップＳ３－８に処理が移行する。

【００５６】ステップＳ３－７においては、セキュリティ管理装置２４は、ゲートウェイ装置１２に対して、フィルタリングの解除命令を出す。この解除命令は、インターネット１８を介して第１のＩＳＰ１６に到達し（図１の（１０）で示される）、第１のＩＳＰ１６からゲートウェイ装置１２に到達する（図１の（１１）で示される）。この解除命令を受けて、ゲートウェイ装置１２はパケット送信者が送信してきたパケットを家庭内ネットワーク１０に供給する。

【００５７】一方、ステップＳ３－８においては、セキュリティ管理装置２４は、不正なアクセスであると判断し、パケットの送信者が接続している第２のＩＳＰ２２に対して、警告を通知する（図１の（１２）で示される）。先に述べたように、このステップＳ３－８において警告が通知されるのは、認証データを所定期間内にセキュリティ管理装置２４が受信できなかった場合、もしくは、認証データが正しくなかった（表中になかった）場合、のいずれかの場合である。

【００５８】以上述べたように、本実施の形態１によれば、家庭内ネットワーク１０にアクセスする権利を有する者に対してのみ家庭内ネットワーク１０への流入を許可することができる。特に、その判断を外部のセキュリティ管理装置２４に委託することができるため、ゲートウェイ装置１２自身の負担を減らすことができるというメリットがある。

【００５９】さらに、不正なアクセスを排除するだけでなく、不正なアクセスがあった場合には、ＩＳＰに対して警告を通知するので、不正行為の抑止効果を期待することができる。

【００６０】セキュリティ管理装置の構成

次に、セキュリティ管理装置２４の構成を図４に基づいて説明する。この図に示すように、セキュリティ管理装置２４は、上述した図２で示す表を管理するゲートウェイ装置１２の個数だけ記憶している記憶手段４０を備えている。また、インターネット１８と接続するためのインターフェース４２を備えている。さらに、図３で説明した動作を実行する制御手段４４を備えている。

【００６１】制御手段４４は、プログラムとそのプログラムを実行するプロセッサとから構成されており、このプログラムによって、上述した各動作の制御が行われる。

【００６２】（１）すなわち、外部のゲートウェイ装置１２から、その自己認証データと、ゲートウェイ装置１２に送信されたパケットのパケット情報と、がインターフェース４２を介してセキュリティ管理装置２４に送信されてきた場合に、そのパケット情報に基づきパケットの送信者に認証データを要求する。そして、認証データを受信する。

【００６３】（２）次に、上記自己認証データからそのゲートウェイ装置１２の表を見つけ、その表中に上記認証データが存在するか否かを検査する。

【００６４】（３）表中に認証データが存在すれば、ゲートウェイ装置１２にパケットに対するフィルタリングを解除し、パケットを家庭内ネットワーク１０に流入することを許可するよう命令する。

【００６５】（４）一方、表中に認証データが存在しない場合や、所定時間内に認証データが送られてこなかった場合には、パケット送信者の管理者に警告を通知する。

【００６６】なお、記憶手段４０は、ハードディスク等の各種の磁気ディスク、又はＣＤＲＯＭ，ＤＶＤＲＯＭ等の各種の光ディスク等、種々の記憶手段を利用することができる。また、セキュリティ管理装置２４は、複数のゲートウェイ装置１２を管理することができる。その場合には、記憶手段４０内に、複数のゲートウェイ装置１２毎に作成された複数の表が格納される。

【００６７】ゲートウェイ装置の構成

次に、ゲートウェイ装置１２の構成を図５に基づいて説明する。この図に示すように、ゲートウェイ装置１２は、家庭内ネットワーク１０に接続するためのインターフェース５０と、インターネット１８に接続するためのインターフェース５２とを備えている。

【００６８】また、ゲートウェイ装置１２は、インターネット１８側からやってきたパケットをフィルタリングするフィルタリング手段５４を備えている。このフィルタリング手段５４は、家庭内ネットワーク１０からインターネット１８に向かうパケットのフィルタリングも行う。

【００６９】ゲートウェイ装置１２は、制御手段５６を有している。この制御手段５６は、フィルタリングの対象となるパケットの定義や、フィルタリングの内容等を設定する手段であり、プログラムとそのプログラムを実行するプロセッサによって構成されている。

【００７０】また、このプログラムによって、制御手段５６は、上述した図３で説明した動作を実行する。

【００７１】（１）すなわち、インターネット１８からパケットがインターフェース５２を介して送信されてきた場合には、そのパケット情報と、自己認証データとを、外部のセキュリティ管理装置２４に送信する。ここで、自己認証データは、ゲートウェイ装置１２を識別可能なデータであればどのようなデータでもかまわない。

【００７２】（２）次に、上記セキュリティ管理装置２４から、フィルタリングの解除命令が送信されてきた場合には、上記フィルタリング手段５４を制御して、家庭内ネットワーク１０への流入を許可するのである。

【００７３】（３）このような解除命令が来ない限り、フィルタリング手段は上記パケットをフィルタリングし続ける。すなわち、家庭内ネットワーク１０への流入を許可しないのである。このようにして不正なアクセスによるパケットの流入を防止することが可能である。

【００７４】なお、フィルタリング手段５４はソフトウェアで構成することも好ましいが、性能を向上（処理速度を向上）させるために、ハードウェアで構成することも好ましい。インターフェース５０，５２はネットワークとのインターフェース手段として既存の構成をそのまま利用可能である。

【００７５】端末の構成

次に、端末２０の構成を図６に基づいて説明する。この図に示すように、端末２０は、第２のＩＳＰ２２と接続するためのインターフェース６０を備えている。

【００７６】また、端末２０は、利用者に所定の情報を表示するための表示手段６２や利用者が情報を入力するための入力手段６４を備えている。これらの表示手段６２や入力手段６４は従来からよく知られた構成である。

【００７７】さらに、端末２０は、制御手段６６を備えている。この制御手段６６は、プログラムとそのプログラムを実行するプロセッサによって構成されている。そして、このプログラムによって、制御手段６６は、上述した図３で説明した動作を実行する。すなわち、制御手段６６は、インターネット１８を介して、セキュリティ管理装置２４から、端末２０の認証データを要求された場合に、その要求に応じて認証データをセキュリティ管理装置２４に送信するのである。

【００７８】実施の形態２

上記実施の形態１では、家庭内ネットワーク１０の例を示したが、プライベートなネットワークであればどのようなネットワークでもかまわない。また、実施の形態１では、インターネット１８の例を示したが、もちろんどのようなネットワークでもかまわない。どのようなネットワークでも本発明を適用することは容易である。

【００７９】また、実施の形態１では、パケットの送信者がＩＳＰを通じてアクセスする場合について説明したが、ＩＳＰを介さずにネットワークに接続する形態でもかまわない。この場合は、管理者としては、ＩＳＰではなく、たとえばその送信者の上司や、送信者の所属する団体等が適切である。セキュリティ管理装置２４は、ＩＳＰの代わりに、これら上司や、団体に対して警告を通知することになる。

【００８０】また、ゲートウェイ装置１２も第１のＩＳＰ１６を介さずに直接ネットワークに接続する形態であっても本発明を同様に適用することが可能である。

【００８１】

【発明の効果】以上述べたように、本発明によれば、外部ネットワークから内部ネットワークへ正当なアクセスのみを許可することができる。また、正当な者からのアクセスか否かを内部ネットワークと外部ネットワークを接続するゲートウェイ装置以外の管理装置に委託することができるため、ゲートウェイ装置の管理負担が減少する。

【００８２】特に、認証データを用いて正当な権利を有するものか否かを判断し、認証データが送信者側から送られてこなかった場合、認証データが不正なものであった場合に、不正アクセスが行われたと判断することができる。

【００８３】また、不正なアクセスであると判断した場

台には、管理者に警告が通知されるため、不正アクセスを将来的にも防止する効果が期待される。また、管理者がインターネットサービスプロバイダである場合には、インターネットサービスプロバイダはそのユーザに不正アクセスを使用とした者がいることを知ることができ、ユーザの管理を強化する効果が得られる。

【0084】さらに、セキュリティ管理装置からの要求に応じて認証データが送信されるように端末装置を構成したので、自己が内部ネットワークに対して正当にアクセスをする権利を有する者であることを容易に証明することができ、外部ネットワークから内部ネットワークへのアクセスを円滑に行うことが可能となる。

【図面の簡単な説明】

【図1】本発明の形態1の通信システムの全体構成図である。

【図2】セキュリティ管理装置に格納されている表の概念図である。

【図3】端末から家庭内ネットワークへのアクセスの動作の流れを表すフローチャートである。

【図4】セキュリティ管理装置の構成ブロック図である。

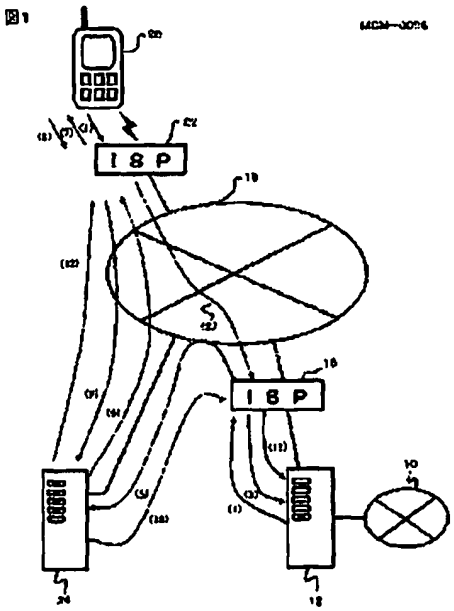
*【図5】ゲートウェイ装置の構成ブロック図である。

【図6】端末の構成ブロック図である。

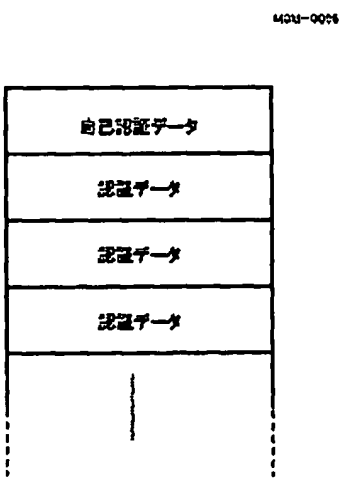
【符号の説明】

10 家庭内ネットワーク
12 ゲートウェイ装置12
16 第1のインターネットサービスプロバイダ
18 インターネット
20 端末
22 第2のインターネットサービスプロバイダ
24 セキュリティ管理装置24
40 記憶手段
42 インターフェース
44 制御手段
50 インターフェース
52 インターフェース
54 フィルタリング手段
56 制御手段
60 インターフェース
62 表示手段
64 入力手段
66 制御手段

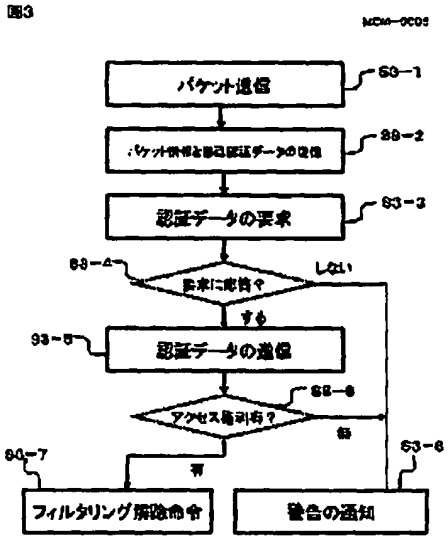
【図1】



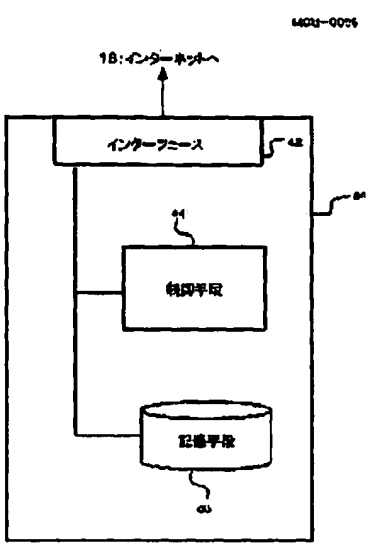
【図2】



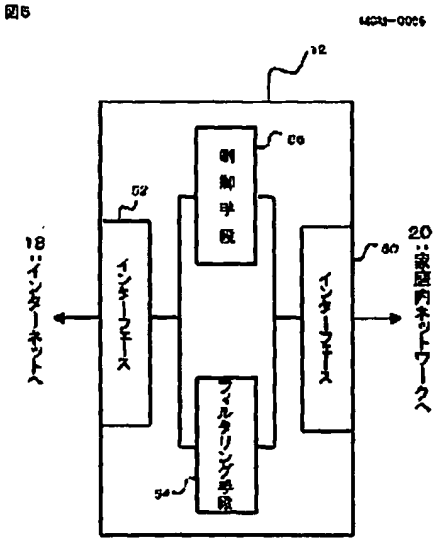
【図3】



【図4】



【図5】



【図6】